AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A data processing apparatus for performing rights processing of content data encrypted with content key data based on usage control policy data, and for decrypting the encrypted content key data, ~~said~~ the data processing apparatus comprising within a tamper-resistant circuit module:

a first bus;

an arithmetic processing circuit connected to ~~said~~ the first bus, for performing the rights processing of the content data based on the usage control policy data;

a storage circuit connected to ~~said~~ the first bus;

a second bus;

a first interface circuit interposed between ~~said~~ the first bus and ~~said~~ the second bus;

an encryption processing circuit connected to ~~said~~ the second bus, for decrypting the content key data;

a hash-value generating circuit that generates hash values of the content data, the content key data, and the usage control policy data;

a public key encryption ~~module~~ circuit that creates signature data using the hash values and verifies the integrity of the signature data ~~performs authentication, creates~~

~~signature data, encrypts and decrypts data for transferring, and shares a session key data obtained by the authentication~~;

a common key encryption ~~module~~ circuit ~~that performs mutual authentication and encrypts and decrypts data by using the session key data~~;

an external bus interface circuit connected to ~~said~~ the second bus; and

a usage monitor;

wherein ~~said~~ the arithmetic processing circuit determines at least one of a purchase mode and a usage mode of the content data based on a handling policy indicated by the usage control policy data, and creates log data which includes a unique identifier of the content data, discount information, and tracing information and indicates result of the determined mode; and the arithmetic processing circuit creates usage control status data in accordance with the determined purchase mode, and controls the use of the content data based on the usage control status data;

~~said~~ the usage control status data comprising a content identification for ~~said~~ the content data, the purchase mode, an identification for ~~said~~ the tamper-resistant circuit module, and a user identification for a user who has purchased ~~said~~ the content data;

wherein the usage monitor monitors ~~said~~ the usage control policy data and ~~said~~ the usage control status data to make sure that ~~said~~ the content data is purchased and used as restricted by ~~said~~ the usage control policy data and ~~said~~ the usage control status data; and

wherein the purchase mode is determined from one or more purchase mode options, and each purchase mode option has a different level of restriction imposed on a playback operation.

2. (Currently Amended) A data processing apparatus according to claim 1, further comprising a second interface circuit within ~~said~~ the tamper-resistant circuit module, wherein ~~said~~ the first bus comprises a third bus connected to ~~said~~ the arithmetic processing circuit and ~~said~~ the storage circuit, and a fourth bus connected to ~~said~~ the first interface circuit, and ~~said~~ the second interface circuit is interposed between ~~said~~ the third bus and ~~said~~ the fourth bus.

3. (Currently Amended) A data processing apparatus according to claim 2, further comprising within ~~said~~ the tamper-resistant circuit module:

a fifth bus;

a third interface circuit connected to ~~said~~ the fifth bus, for performing communication with a data processing circuit having an authentication function which is loaded on one of a recording medium and an integrated circuit card; and

a fourth interface circuit interposed between ~~said~~ the fourth bus and ~~said~~ the fifth bus.

4. (Canceled)

5. (Currently Amended) A data processing apparatus according to claim 4, wherein:

~~said~~ the storage circuit stores private key data of ~~said~~ the data processing apparatus and public key data of a second data processing apparatus;

~~said~~ the public-key encryption circuit verifies the integrity of ~~signature data, which verifies the integrity of the content data, the content key data, and~~ the usage control policy data, by using the public key data, and when recording the content data, the content key data, and the usage control policy data on a recording medium or when sending the content data, the content key data, and the usage control policy data to ~~said~~ the second data processing apparatus, ~~said~~ the public-key encryption circuit creates the signature data, which verifies the integrity of the content data, the content key data, and the usage control policy data, by using the private key data; and

~~said~~ the common-key encryption circuit decrypts the content key data, and when sending the content data, the content key data, and the usage control policy data to ~~said~~ the second data processing apparatus online, ~~said~~ the common-key encryption circuit encrypts and decrypts the content data, the content key data, and the usage control policy data by using session key data obtained by performing mutual authentication with ~~said~~ the second data processing apparatus.

6. (Canceled)

7. (Currently Amended) A data processing apparatus according to claim 1, further comprising a random-number generating circuit within ~~said~~ the tamper-resistant circuit module, ~~said~~ the random-number generating circuit being connected to ~~said~~ the second bus, for generating a random number for performing mutual authentication with a second data processing apparatus when sending the content data, the content key

data, and the usage control policy data to ~~said~~ the second data processing apparatus online.

8. (Currently Amended) A data processing apparatus according to claim 1, wherein ~~said~~ the external bus interface circuit is connected to an external storage circuit for storing at least one of the content data, the content key data, and the usage control policy data.

9. (Currently Amended) A data processing apparatus according to claim 8, further comprising a storage-circuit control circuit for controlling access to ~~said~~ the storage circuit and access to ~~said~~ the external storage circuit via ~~said~~ the external bus interface circuit in accordance with a command from ~~said~~ the arithmetic processing circuit.

10. (Currently Amended) A data processing apparatus according to claim 1, wherein ~~said~~ the external bus interface circuit is connected to a host arithmetic processing apparatus on which ~~said~~ the data processing apparatus is loaded.

11. (Currently Amended) A data processing apparatus according to claim 8, further comprising a storage management circuit for managing an address space of ~~said~~ the storage circuit and an address space of ~~said~~ the external storage circuit.

12-14. (Canceled)

15. (Currently Amended) A data processing apparatus according to claim 4, wherein, when the content key data is encrypted with license key data having an effective period, ~~said~~ the storage circuit stores the license key data, ~~said~~ the data processing apparatus further comprises a real time clock for generating real time, ~~said~~ the arithmetic processing circuit reads the effective license key data from ~~said~~ the storage circuit based on the real time indicated by ~~said~~ the real time clock, and ~~said~~ the common-key encryption circuit decrypts the content key data by using the read license key data.

16. (Currently Amended) A data processing apparatus according to claim 1, wherein ~~said~~ the storage circuit writes and erases data in units of blocks, and ~~said~~ the data processing apparatus comprises within ~~said~~ the tamper-resistant circuit module, a write-lock control circuit for controlling the writing and erasing of the data into and from ~~said~~ the storage circuit in units of blocks under the control of ~~said~~ the arithmetic processing circuit.

17. (Currently Amended) A data processing apparatus for performing rights processing of content data encrypted with content key data based on usage control policy data, and for decrypting the encrypted content key data, ~~said~~ the data processing apparatus comprising within a tamper-resistant circuit module:

a first bus;

an arithmetic processing circuit connected to ~~said~~ the first bus, for performing the rights processing of the content data based on the usage control policy data;

a storage circuit connected to ~~said~~ the first bus;

a second bus;

an interface circuit interposed between ~~said~~ the first bus and ~~said~~ the second bus;

an encryption processing circuit connected to ~~said~~ the second bus, for decrypting the content key data;

a hash-value generating circuit that generates hash values of the content data, the content key data, and the usage control policy data;

a public key encryption ~~module~~ circuit that creates signature data using the hash values and verifies the integrity of the signature data ~~performs authentication, creates signature data, encrypts and decrypts data for transferring, and shares a session key data obtained by the authentication~~;

a common key encryption ~~module~~ circuit ~~that performs mutual authentication and encrypts and decrypts data by using the session key data~~;

an external bus interface circuit connected to ~~said~~ the second bus; and

a usage monitor;

wherein, upon receiving an interrupt from an external circuit via ~~said~~ the external bus interface circuit, ~~said~~ the arithmetic processing circuit becomes a slave for ~~said~~ the external circuit so as to perform processing designated by the interrupt, and reports a result of the processing to ~~said~~ the external circuit;

wherein ~~said~~ the arithmetic processing circuit determines at least one of a purchase mode and a usage mode of the content data based on a handling policy indicated by the usage control policy data, and creates log data which includes a unique identifier of the content data, discount information, and tracing information and indicates a result of the determined mode; and the arithmetic processing circuit creates usage control status data in accordance with the determined purchase mode, and controls the use of the content data based on the usage control status data;

~~said~~ the usage control status data comprising a content identification for ~~said~~ the content data, the purchase mode, an identification for ~~said~~ the tamper-resistant circuit module, and a user identification for a user who has purchased ~~said~~ the content data;

wherein the usage monitor monitors ~~said~~ the usage control policy data and ~~said~~ the usage control status data to make sure that ~~said~~ the content data is purchased and used as restricted by ~~said~~ the usage control policy data and ~~said~~ the usage control status data; and

wherein the purchase mode is determined from one or more purchase mode options, and each purchase mode option has a different level of restriction imposed on a playback operation.

18. (Currently Amended) A data processing apparatus according to claim 17, wherein ~~said~~ the arithmetic processing circuit reports the result of the processing by outputting an interrupt to ~~said~~ the external circuit.

19. (Currently Amended) A data processing apparatus according to claim 17, wherein ~~said~~ the external bus interface comprises a common memory for ~~said~~ the arithmetic processing circuit and ~~said~~ the external circuit, and ~~said~~ the arithmetic processing circuit writes the result of the processing into ~~said~~ the common memory, and ~~said~~ the external circuit obtains the result of the processing by polling.

20. (Currently Amended) A data processing apparatus according to claim 19, wherein ~~said~~ the external bus interface comprises:

a first status register indicating an execution status of the processing requested from ~~said~~ the external circuit in ~~said~~ the arithmetic processing circuit, and including a flag set by ~~said~~ the arithmetic processing circuit and read by ~~said~~ the external circuit;

a second status register indicating whether ~~said~~ the external circuit has requested ~~said~~ the arithmetic processing circuit to perform processing, and including a flag set by ~~said~~ the external circuit and read by ~~said~~ the arithmetic processing circuit; and

~~said~~ the common memory for storing a result of the processing.

21. (Currently Amended) A data processing apparatus according to claim 18, wherein ~~said~~ the storage circuit stores an interrupt program describing the processing designated by the interrupt, and ~~said~~ the arithmetic processing circuit performs the processing by executing the interrupt program read from ~~said~~ the storage circuit.

22. (Currently Amended) A data processing apparatus according to claim 21, wherein ~~said~~ the storage circuit stores a plurality of ~~said~~ the interrupt programs, and a plurality of sub-routines to be read when executing the interrupt program, and ~~said~~ the arithmetic processing circuit appropriately reads and executes the sub-routines from ~~said~~ the storage circuit when executing the interrupt program read from ~~said~~ the storage circuit.

23-56. (Canceled)

57. (Currently Amended) A data processing method of performing rights processing for content data encrypted with content key data based on usage control policy data, and of decrypting the encrypted content key data, ~~said~~ the data processing method comprising the steps of:

determining at least one of a purchase mode and a usage mode of the content data based on a handling policy indicated by the usage control policy data;

creating log data which includes a unique identifier of the content data, discount information, and tracing information and indicates a result of the determined purchase mode;

creating usage control status data in accordance with the determined purchase mode; ~~said~~ the usage control status data comprising a content identification for ~~said~~ the content data, the purchase mode, an identification for a tamper-resistant circuit module, and a user identification for a user who has purchased ~~said~~ the content data;

monitoring ~~said~~ the usage control policy data and ~~said~~ the usage control status data to make sure that ~~said~~ the content data is purchased and used as restricted by ~~said~~ the usage control policy data and ~~said~~ the usage control status data;

controlling the use of the content data based on the usage control status data;

recording the content data, for which the purchase mode is determined, on a recording medium; [[and]]

generating hash values of the content data, the content key data, and the usage control policy data

performing authentication;

creating a signature data using the hash values;

verifying the integrity of the signature data;

sharing session key data obtained by the authentication; and

encrypting the content key data and the usage control status data by using the session key data;

wherein the purchase mode is determined from one or more purchase mode options, and each purchase mode option has a different level of restriction imposed on a playback operation.